FortiAuthenticator - RADIUS Accounting Proxy Configuration Guide

VERSION 1.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

06/10/2015

FortiAuthenticator 4.0 - RADIUS Accounting Proxy Configuration Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
2012-12-05	Initial release.

About this document

This document introduces the FortiAuthenticator RADIUS Accounting Proxy and it can be configured for use in a FortiGate or FortiMail environment. The document covers the configuration of the FortiAuthenticator only. Please see the FortiOS and FortiMail Admin Guides for details of how to configure those specific solutions.

Software versions

The configuration discussed in this document was tested on the following firmware versions:

- FortiAuthenticator 2.0 GA
- FortiOS 5.0 GA
- FortiMail 4.3

FortiAuthenticator RADIUS Accounting Proxy

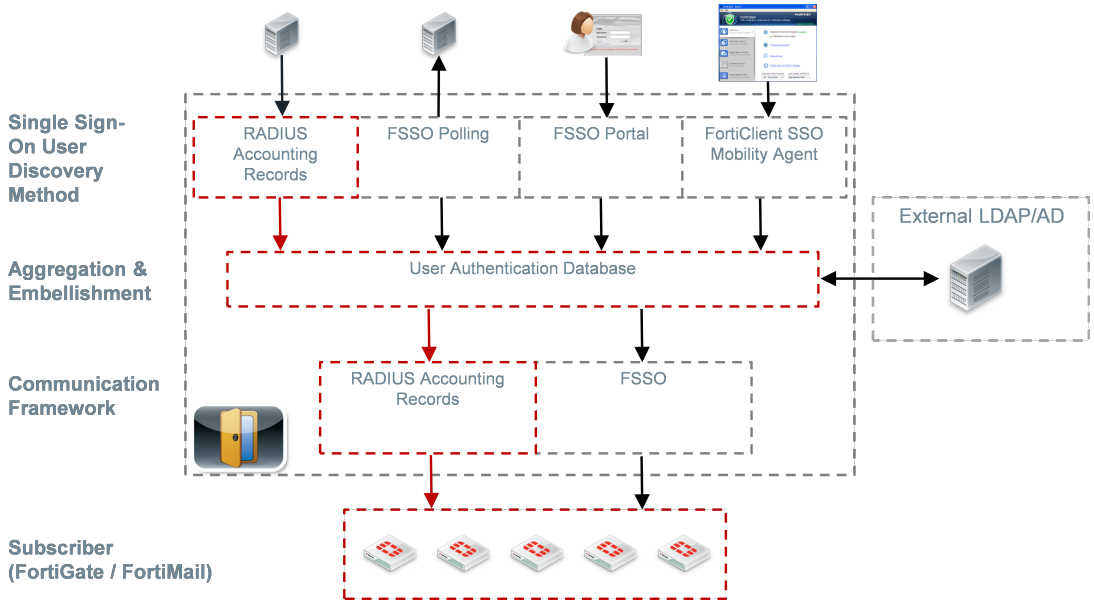
The FortiAuthenticator SSO Framework

In addition to explicit RADIUS and LDAP authentication, FortiAuthenticator supports the gathering of authentication state from external systems and the sharing with FortiGate (and in some cases FortiMail) for use in Identity Based Policies. Login events are gathered using multiple techniques and shared using one of two communications methods:

FSSO: Fortinet Single Sign-on

RSSO: RADIUS Single Sign-on using Attributes from RADIUS Accounting records.

Note that this document only covers the use of RADIUS Accounting Records for single sign-on. The use of FortiAuthenticator with FSSO authentication methods and communication is documented in the FortiAuthenticator FSSO Authentication Methods Guide https://docs.fortinet.com/auth.html



There are four layers within the FortiAuthenticator SSO framework:

Discovery Methods:	Methods in which the user identity and their location (IP) are discovered

Aggregation and Embellishment:	Collection of user identity and addition of any missing information (e.g. group)
Communication Framework:	Method by which the authentication information is communicated with the subscribing device
Subscriber:	Device that subscribes to the FortiAuthenticator FSSO feed

For the purpose of this document, only the flow shown in Red will be considered.

Introduction to RADIUS Accounting Proxy Authentication

RADIUS Accounting Proxy based authentication relies on the administrator configuring their existing RADIUS server to send Fortinet specific RADIUS AVP (Attribute Value Pairs) to each of the FortiGate?FortiMail devices requiring the login information. This is then used to identify and authenticate the user in future connections.

The drawback of this is that often, as the RADIUS Server is business critical, changes to the server are strictly limited. Additionally, in some cases, accounting records can only be sent to a single endpoint, not multiple endpoints as is required.

The FortiAuthenticator RADIUS Accounting Proxy functionality has been designed to overcome these limitations by proxying the RADIUS accounting records, modifying and replicating them to the multiple subscribing endpoints it in the process.

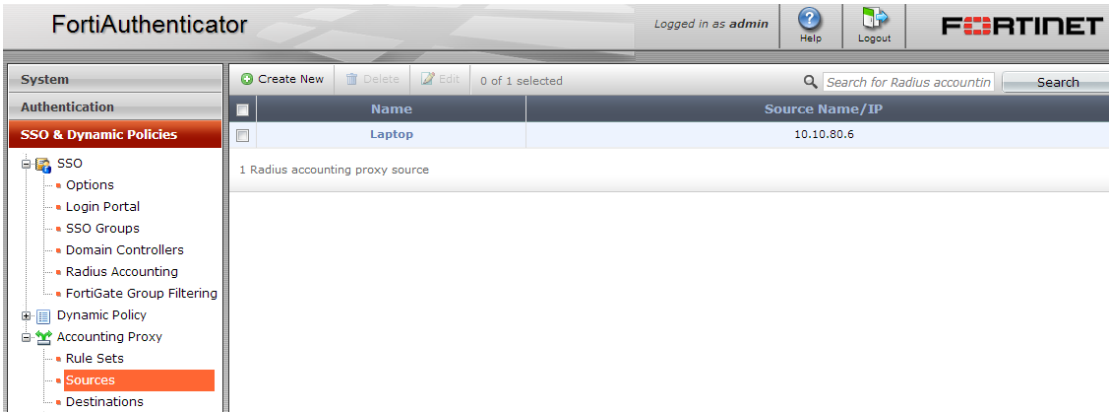
The following terminology is used throughout this document:

Source:	The source of the RADIUS Accounting records. This will be the existing RADIUS Server.
Destination:	The destination of the RADIUS Accounting records. This is one or more subscriber endpoints; FortiGate or FortiMail devices which will use the records for the purpose of identifying the users and their traffic.

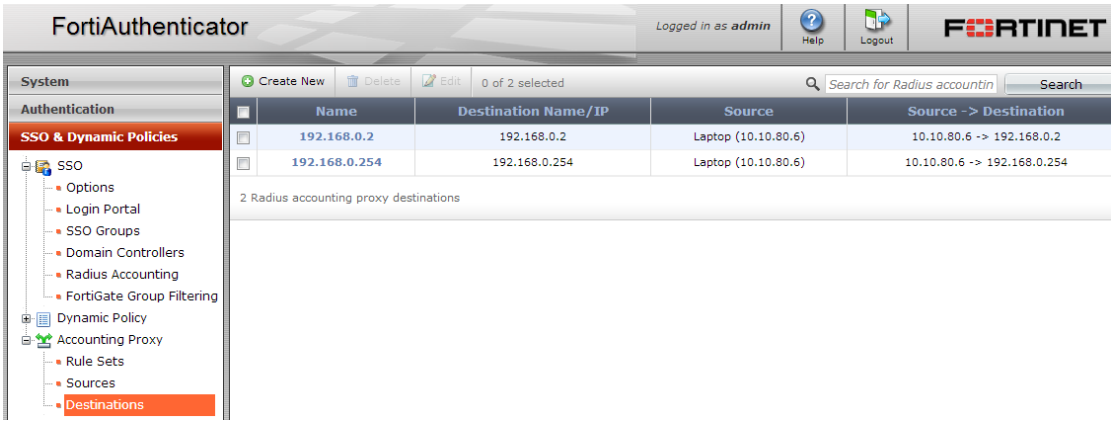
Configuring the FortiAuthenticator

The RADIUS Accounting Proxy is configured via *SSO & Dynamic Policies→Accounting Proxy*. All other references to RADIUS, for example in the *SSO & Dynamic Policies→SSO* section are related to FSSO and should be avoided. See the FortiAuthenticator FSSO Authentication Methods Guide http://docs.fortinet.com/d/fortiauthenticator-fsso-authentication-methods-configuration-guide-1 for more information on these methods.

1. Browse to *SSO & Dynamic Policies* > *Accounting Proxy* > *Sources* and configure an accounting source. This is usually the RADIUS server but the example below uses a laptop running NTRADPing for test purposes.

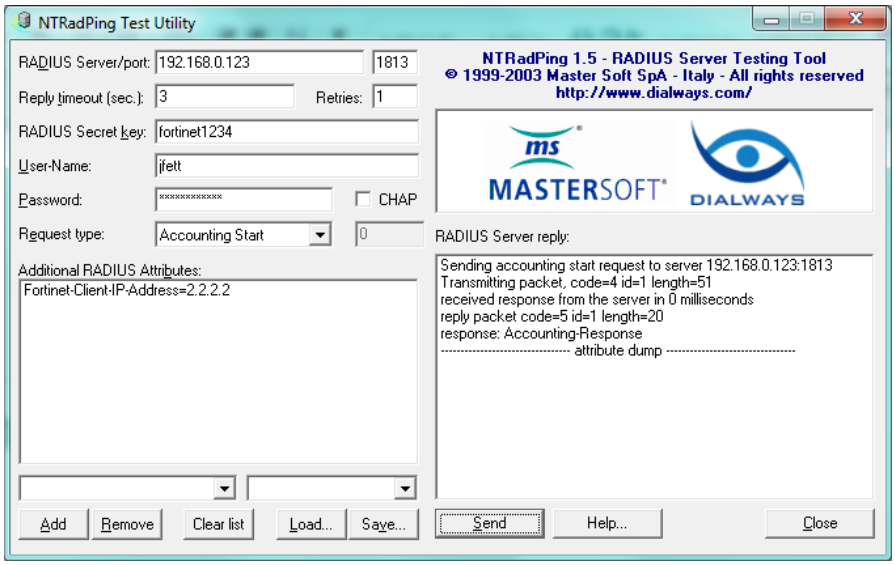


2. Browse to *SSO & Dynamic Policies* > *Accounting Proxy* > *Destinations* and configure a list of accounting destinations. This is the list of FortiGate or FortiMail devices which will be using RADIUS Accounting for user identification and authentication.



Sending RADIUS Accounting packets to the FortiAuthenticator from a RADIUS server will result in a login event being triggered on the FortiAuthenticator.

No authentication login state is maintained (unlike with the FSSO method) therefore the user will not appear in *Monitor* > *SSO* > *SSO Users*.



To verify the RADIUS packets are being “broadcast” to the destination endpoints, traffic sniffing can be employed.

Original RADIUS Accounting Packet

21:51:54.410474 IP 10.10.80.6.54007 > 192.168.0.123.1813: RADIUS, Accounting Request (4), id: 0x01 length: 51

0x0000: 4500 004f 6b93 0000 7f11 b4d7 0a0a 5006 E..Ok.....P.

0x0010: c0a8 007b d2f7 0715 003b f4dc 0401 0033 ...{.....;.....3

0x0020: 6515 7df6 6219 f4d5 9b4f 790f ec1d bdb9 e.}.b....Oy.....

0x0030: 0107 6a66 6574 7428 0600 0000 012c 0635 ..jfett(.....,.5

0x0040: 3639 361a 0c00 0030 4402 0602 0202 0200 696....0D.....

0x0050: 0000 00 ...

21:51:54.410885 IP 192.168.0.123.1813 > 10.10.80.6.54007: RADIUS, Accounting Response (5), id: 0x01 length: 20

0x0000: 4500 0030 f5e0 0000 4011 69a9 c0a8 007b E..0....@.i....{

0x0010: 0a0a 5006 0715 d2f7 001c 45e4 0501 0014 ..P.....E.....

0x0020: 3af2 e152 3f8f bbe7 8794 3e61 09bb d80f :..R?.....>a....

Duplicated RADIUS Accounting Packets send to Destination Endpoints (FGT/FML)

21:51:54.411266 IP 192.168.0.123.33323 > 192.168.0.254.1813: RADIUS, Accounting Request (4), id: 0xf6 length: 57

0x0000: 4500 0055 7b40 0000 4011 7c8e c0a8 007b E..U{@..@.|....{

0x0010: c0a8 00fe 822b 0715 0041 04d8 04f6 0039 .....+...A.....9

```
0x0020:  0c96 96a0 0e5e aabd 01fd 675b fa81 f9da  .....^....g[....
0x0030:  0107 6a66 6574 7428 0600 0000 012c 0635  ..jfett(.....,.5
0x0040:  3639 361a 0c00 0030 4402 0602 0202 0204  696....0D.......
0x0050:  060a 0a50 06                             ...P.
21:51:54.411499 IP 192.168.0.123.33324 > 192.168.0.2.1813: RADIUS, Accounting Request (4), id: 0xc1
length: 57
0x0000:  4500 0055 1cdd 0000 4011 dbed c0a8 007b  E..U....@......{
0x0010:  c0a8 0002 822c 0715 0041 66f0 04c1 0039  .....,...Af....9
0x0020:  de5a fa38 bc5c 7d07 f898 6f5c 71e7 6d4a  .Z.8.\}...o\q.mJ
0x0030:  0107 6a66 6574 7428 0600 0000 012c 0635  ..jfett(.....,.5
0x0040:  3639 361a 0c00 0030 4402 0602 0202 0204  696....0D.......
0x0050:  060a 0a50 06                             ...P.
```

Rule Sets

In situations where changes to the RADIUS infrastructure are restricted, it may not be possible to define the explict attributs recommended by Fortinet and differing attributes may be required. FortiAuthenticator supports the mapping of existing attributes and addition of new attributes with dynamic values.

To create a new rule set:

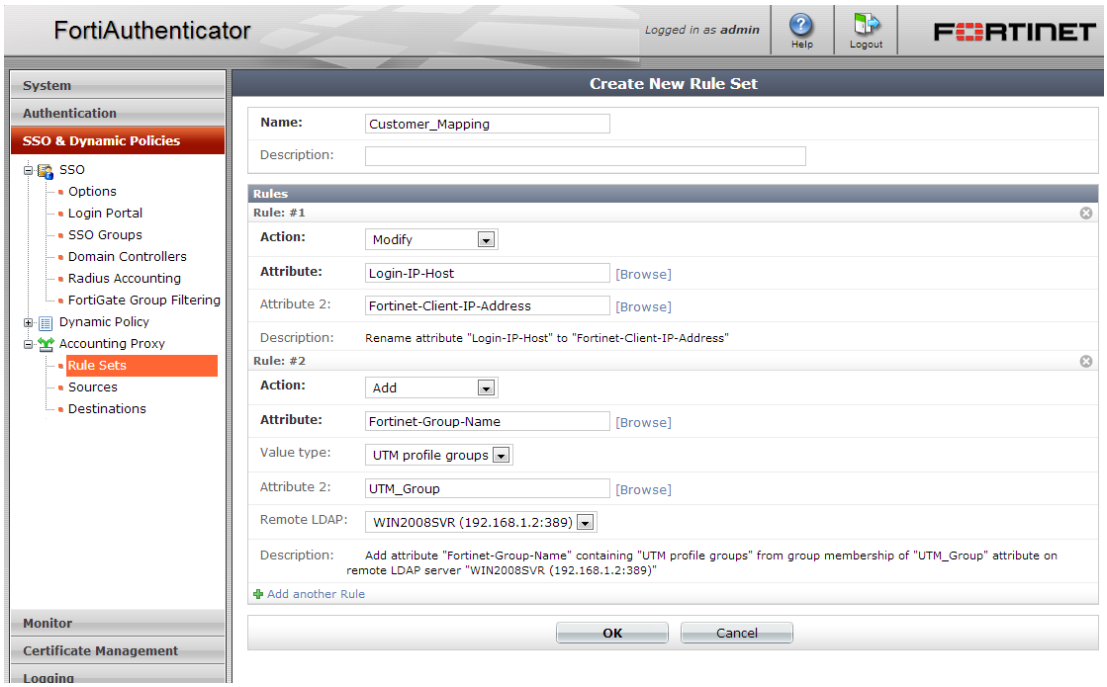
- Browse to *SSO & Dynamic Policies* > *Accounting Proxy* > *Rule Sets*.

Attribute modification

- Select *Action*: ***Modify*** and select the source Attribute (*Attribute 1*) and Destination attribute (*Attribute 2*).

Attribute addition

1. Select *Action*: ***Add*** and select the Attribute you wish to create (*Attribute 1*).
2. Select the type of attribute you wish to create e.g a dynamic attribute such as UTM_Group or a static value.
3. Specify the LDAP server and query to pull the relevant values from LDAP.


FortiAuthenticator
Logged in as admin
Help
Logout
FORTINET
System
Authentication
SSO & Dynamic Policies
SSO
Options
Login Portal
SSO Groups
Domain Controllers
Radius Accounting
FortiGate Group Filtering
Dynamic Policy
Accounting Proxy
Rule Sets
Sources
Destinations
Monitor
Certificate Management
Logging
Create New Rule Set
Name: Customer_Mapping
Description:
Rules
Rule: #1
Action: Modify
Attribute: Login-IP-Host [Browse]
Attribute 2: Fortinet-Client-IP-Address [Browse]
Description: Rename attribute "Login-IP-Host" to "Fortinet-Client-IP-Address"
Rule: #2
Action: Add
Attribute: Fortinet-Group-Name [Browse]
Value type: UTM profile groups
Attribute 2: UTM_Group [Browse]
Remote LDAP: WIN2008SVR (192.168.1.2:389)
Description: Add attribute "Fortinet-Group-Name" containing "UTM profile groups" from group membership of "UTM_Group" attribute on remote LDAP server "WIN2008SVR (192.168.1.2:389)"
Add another Rule
OK
Cancel

Appendix A – Debugging RADIUS Accounting

To test RADIUS Accounting and verify correct configuration, it is most simple initially to test with desktop tools such as NTRADPing (provided by http://www.mastersoft-group.com/download/).

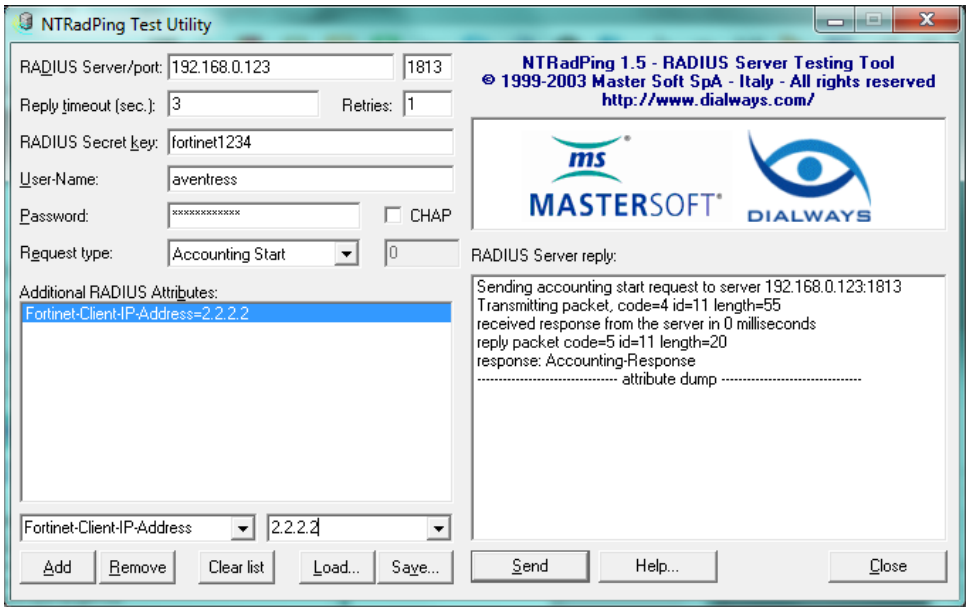
Once downloaded and installed, follow the instructions to install the Fortinet RADIUS Dictionary into the application.

To trigger a login into FSSO, the RADIUS packet must contain:

```
User-Name: <User name>
```

```
Fortinet-Client-IP-Address: <Client IP>
```

To replicate sending these attributes, configure the NTRADPing software as shown:



- Take care to ensure the RADIUS Port is changed to 1813 and the Request type is set to Accounting Start.
- It is not necessary to add an AVP for User-Name as it is specified in the explicit User-name field.
- If successful, FortiAuthenticator will acknowledge the receipt of the packet and the NTRADPing client will display this success with “Accounting-Response”.
- If this is not successful, verify that UDP/1813 can pass to the FortiAuthenticator and that the RADIUS Secret Key is configured correctly on both sides.

Authentication may be successful but the user not found in LDAP (or LDAP is not configured correctly). In this case the login will be received but the record dropped due to lack of group info.

Appendix B – RADIUS Dictionary

```
#####################################################################
#
#
# Fortinet, Inc. #
#
#
# RADIUS VSA Dictionary #
#
#
# This RADIUS dictionary is to be used in conjunction #
# with FortiOS v4.0.0. #
#
#
# Copyright 2009 #
#
#
# Technical Support
#
# http://www.fortinet.com/support #
#
#
#####################################################################
VENDOR Fortinet 12356
BEGIN-VENDOR Fortinet
ATTRIBUTE Fortinet-Group-Name 1 string
ATTRIBUTE Fortinet-Client-IP-Address 2 ipaddr
ATTRIBUTE Fortinet-Vdom-Name 3 string
ATTRIBUTE Fortinet-Client-IPv6-Address 4 octets
ATTRIBUTE Fortinet-Interface-Name 5 string
ATTRIBUTE Fortinet-Access-Profile 6 string
#
# Integer Translations
#
END-VENDOR Fortinet
```